ABSTRACT OF THE DISCLOSURE

A method and apparatus for performing cryptographic computations employing recursive algorithms to accelerate multiplication and squaring operations. Products and squares of long integer values are recursively reduced to a combination of products and squares reduced-length integer values in a host processor. The reduced-length integer values are passed to a co-processor. The values may be randomly ordered to prevent disclosure of secret data.